

IN THE CLAIMS:

Please amend Claims 1, 7, 13, 16 and 19 as follows.

1. (Currently Amended) An authentication apparatus having a plurality of authentication mechanisms, characterized by comprising:

an input unit adapted to input authentication information of an object of authentication, said authentication information having been already authenticated by a first mechanism that is in use;

a determination unit adapted to determine whether the authentication information that has been input by said input unit corresponds to an object of authentication that has an authority to change over the first authentication mechanism in use to another authentication mechanism;

a display control unit adapted to display a list of the plurality of authentication mechanisms if it has been determined by said determination unit that the authentication information that has been input corresponds to the object of authentication that has the authority to make the changeover;

a registration unit adapted to register, as an effective authentication mechanism, a second authentication mechanism that has been selected from the list displayed by said display control unit;

a verification unit adapted to verify that authentication of the object of authentication in the second authentication mechanism succeeds; and

a changeover control an invalidation unit adapted to control management of the object of authentication so that successful authentication of the object of authentication in the second authentication mechanism is verified before management is changed over from the first authentication mechanism to the second authentication mechanism, wherein the object of authentication continues to be in an authenticated state in the first authentication mechanism, and is not released from management under the first authentication mechanism, until successful

~~authentication in the second authentication mechanism is verified invalidate the first authentication mechanism if it has been verified by the verification unit that the authentication of the object of authentication in the second authentication mechanism succeeds, and not to invalidate the first authentication mechanism if it has not been verified by the verification unit that the authentication of the object of authentication in the second authentication mechanism succeeds.~~

2. (Canceled)

3. (Previously Presented) The authentication apparatus according to claim 1, wherein said input unit reads a card on which authentication information of an object of authentication has been recorded and inputs said authentication information.

4. (Previously Presented) The authentication apparatus according to claim 1, wherein said input unit inputs the authentication information using a web browser.

5. (Previously Presented) The authentication apparatus according to claim 1, wherein each of said plurality of authentication mechanisms has:

a storage unit that has registered authentication information of an object of authentication; and

an authentication determination unit which, in a case where entered authentication information of a user has been registered in said storage unit, is for authenticating this object of authentication.

6. (Previously Presented) The authentication apparatus according to claim 1, further having a start-up unit for starting up an authentication mechanism that has been registered as an effective authentication mechanism by said registration unit.

7. (Currently Amended) An authentication method of changing over a plurality of authentication mechanisms and performing authentication with any one of said plurality of authentication mechanisms, comprising:

an input step of inputting authentication information of an object of authentication, said authentication information having been already authenticated by a first authentication mechanism that is in use;

a determination step of determining whether the authentication information that has been input at said input step corresponds to an object of authentication that has an authority to change over the first authentication mechanism in use to another authentication mechanism;

a display control step of displaying a list of the plurality of authentication mechanisms if it has been determined at said determination step that the authentication information that has been input corresponds to the object of authentication that has the authority to make the changeover;

a registration step of registering, as an effective authentication mechanism, a second authentication mechanism that has been selected from the list displayed at said display control step;

a verification step of verifying that authentication of the object of authentication in the second authentication mechanism succeeds; and

an invalidation a changeover control step of controlling management of the object of authentication so that successful authentication of the object of authentication in the second authentication mechanism is verified before management is changed over from the first authentication mechanism to the second authentication mechanism, wherein the object of authentication continues to be in an authenticated state in the first authentication mechanism, and

~~is not released from management under the first authentication mechanism, until successful authentication in the second authentication mechanism is verified, invalidating the first authentication mechanism[[3]] if it has been verified in the verification step that the authentication of the object of authentication in the second authentication mechanism succeeds, and not invalidating the first authentication mechanism if it has not been verified at the verification step that the authentication of the object of authentication in the second authentication mechanism succeeds~~

~~wherein one or more of the foregoing steps is performed using a processor.~~

8. (Canceled)

9. (Previously Presented) The authentication method according to claim 7, wherein a card on which authentication information of an object of authentication has been recorded is read and said authentication information is input at said input step.

10. (Previously Presented) The authentication method according to claim 7, wherein the authentication information input by a web browser at said input step.

11. (Previously Presented) The authentication method according to claim 7, wherein each of said plurality of authentication mechanisms has a storage unit that registers authentication information of an object of authentication, and said method further has an authentication determination step which, in a case where entered authentication information of an object of authentication has been registered in said storage unit, is a step of authenticating this object of authentication.

12. (Previously Presented) The authentication method according to claim 7, further having a start-up step of starting up an authentication mechanism that has been registered as an effective authentication mechanism at said registration step.

13. (Currently Amended) An authentication method comprising:

an input step of inputting authentication information of an object of authentication;

a first authentication step of authenticating whether an object of authentication has access right to a first system using the authentication information of the object of authentication that has been input at said input step, and allowing the object of authentication to access the first system if authentication succeeds;

a second authentication step of authenticating whether the object of authentication has access right to a second system using the authentication information of the object of authentication that has been input at said input step, and allowing the object of authentication to access the second system if authentication succeeds;

a control step of controlling whether the object of authentication will be managed under management of the first system or under management of the second system; and

a verification step of verifying that authentication of the object of authentication in the second system has succeeded at said second authentication step;

wherein if an instruction is recognized, that instructs to switch the object of authentication that is authenticated at the first authentication step from management under the first system to management under the second system, has been recognized, said control step performs control so that successful authentication of the object of authentication in the second system is verified before management is changed over from the first system to the second system, wherein the object of authentication continues to be in an authenticated state in the first system, and is not released from management in the first system, until successful authentication in the second system is verified, and

wherein one or more of the above steps is performed using a processor controls said first authentication step and said second authentication step, in order to switch the object of authentication from management under the first system to management under the second system if the authentication of the object of authentication at said second authentication step has been

verified at said verification step, and in order not to switch the object of authentication from management under the first system to management under the second system, if the authentication of the object of authentication at said second authentication step has not been verified at said verification step.

14. (Previously Presented) The authentication method according to claim 13, wherein said control step controls said first authentication step in such a manner that the object of authentication is excluded from management at said first authentication step in a case where it is verified at said verification step that the object of authentication has been authenticated at said second authentication step.

15. (Previously Presented) The authentication method according to claim 13 wherein said first authentication step authenticates user-level access privilege, and said second authentication step manages administrator-level access privilege.

16. (Currently Amended) An authentication apparatus comprising:

- an input unit adapted to input authentication information of an object of authentication;
- a first authentication unit adapted to authenticate whether an object of authentication has access right to a first system using the authentication information of the object of authentication that has been input by said input unit, and allowing the object of authentication to access the first system if authentication succeeds;
- a second authentication unit adapted to authenticate whether the object of authentication has access right to a second system using the authentication information of the object of authentication that has been input by said input unit, and allowing the object of authentication to access the second system if authentication succeeds;
- a control unit adapted to control whether the object of authentication will be managed under management of the first system or under management of the second system; and

a verification unit adapted to verify that authentication of the object of authentication in the second system by said second authentication unit has succeeded;

wherein if an instruction is recognized, that instructs to switch the object of authentication that is authenticated at the first authentication step from management under the first system to management under the second system ~~has been recognized~~, said control unit performs control so that successful authentication of the object of authentication in the second system is verified before management is changed over from the first system to the second system, wherein the object of authentication continues to be in an authenticated state in the first system, and is not released from management in the first system, until successful authentication in the second system is verified ~~controls said first authentication unit and said second authentication unit, in order to switch the object of authentication from management under the first system to management under the second system if the authentication of the object of authentication by said second authentication unit has been verified by said verification unit, and in order not to switch the object of authentication from management under the first system to management under the second system, if the authentication of the object of authentication by said second authentication unit has not been verified by said verification unit.~~

17. (Previously Presented) The authentication apparatus according to claim 16, wherein said control unit controls said first authentication unit in such a manner that the object of authentication is excluded from management by said first authentication unit in a case where it is verified by said verification unit that the object of authentication has been authenticated by said second authentication unit.

18. (Previously Presented) The authentication apparatus according to claim 16 wherein said first authentication unit authenticates user-level access privilege, and said second authentication unit manages administrator-level access privilege.

19. (Currently Amended) An authentication program stored in a computer-readable storage medium comprising:

code for implementing an input step of inputting authentication information of an object of authentication;

code for implementing a first authentication step of authenticating whether an object of authentication has access right to a first system using the authentication information of the object of authentication that has been input at said input step, and allowing the object of authentication to access the first system if authentication succeeds;

code for implementing a second authentication step of authenticating whether the object of authentication has access right to a second system using the authentication information of the object of authentication that has been input at said input step, and allowing the object of authentication to access the second system if authentication succeeds;

code for implementing a control step of controlling whether the object of authentication will be managed under management of the first system or under management of the second system; and

code for implementing a verification step of verifying that authentication of the object of authentication in the second system has succeeded at said second authentication step;

wherein if an instruction is recognized, that switches the object of authentication that is authenticated at the first authentication step from management under the first system to management under the second system, ~~has been re-recognized~~, said control step performs control so that successful authentication of the object of authentication in the second system is verified before management is changed over from the first system to the second system, wherein the object of authentication continues to be in an authenticated state in the first system, and is not released from management in the first system, until successful authentication in the second system is verified controls said first authentication step and said second authentication step, in order to switch the object of authentication from management under the first system to management under the second system if the authentication of the object of authentication at said second authentication step has been verified at said verification step, and in order not to switch

~~the object of authentication from management under the first system to management under the second system, if the authentication of the object of authentication at said second authentication step has not been verified at said verification step.~~